Appendix H

Applications Security Checklist

DCE Application Development Guidance

Item	Guidance	Rationale
1	Determine the level of security required for each client/server pair.	
2	Write an ACL manager for each server.	
3	Use DCE access control lists to protect distributed files.	
4	Generate an ACL for each server listing all principals for the server objects and the types of access allowed.	
5	Use DCE auditing to audit DCE applications according to the business rules or security policy of the application.	
6	Design appropriate level of security into DCE application. The application controls its own security levels.	
7	Authorization: TBD.	
8	Design appropriate level of security into DCE application.	
9	Data protection: TBD.	
10	Authentication: Use the DCE client/server authentication mechanisms. Use one of the following options: a) Use a transparent DCE wrapper. b) Use the DCE GSSAPI.	a) Don't use the rsh or rexec and trusted hosts mechanism (i.e., hosts.equiv or .rhost files) for client/server communication. b) In using the GSSAPI, the client application obtains a user credential and the server verifies the user credential through another call to the GSSAPI. The client may pass the credential during the first message to the server, but preferably the credential will be passed

during each interchange.

11 Revise the application to use an authenticated DCE RPC. Guidance for developing DCE RPC applications is contained in the Distributed Computing Environment (DCE) Applications Programming Guide for GCCS Version 1.0.

Oracle Application Development Guidance

Item	Guidance	Rationale
1	The redo log is used in the ARCHIVELOG mode.	If the redo log is operated in ARCHIVELOG mode, additional backups of redo log are not necessary.
2	Turn on mirrored redo log.	Maintains two or more copies of the redo log on different disks.
3	Use the mirrored control files feature.	The control files are used to guide the progression of the recovery procedure. The control files keep information about the file structure of the database and the current log sequence being written by the LGWR.
4	Perform partial backups of datafiles and control files frequently.	The database can be completely recovered from both instance and disk failure. Also the database can be backed up while it is open and available for use.
5	Perform full backups periodically. Note: The database has to be closed and unavailable to perform full backups.	
6	Use the system tablespace only for the data dictionary.	
7	Create a new Oracle instance for each application running on the same DBMS.	Ensures that each application has its own set of control files and datafiles. Note: If there is more than one application on the same host, having separate instance for each may lead to performance degradation.
8	Each database within an application has its own tablespace.	This will ensure that each database will have its own set of datafiles.

9	Use Views and Stored Procedures.	Restricts direct access to tables.
10	Restrict the use of DELETE cascade when defining referential constraints.	Delete cascade action specifies that when rows containing referenced parent key values are deleted, all rows in the child tables with dependent foreign key values are also deleted.
11	Application tables are not created under the "system" account.	Access to the "system" account should be restricted.

Sybase Application Development Guidance

Item	Guidance	Rationale
1	Disk mirroring is used for rapid recovery.	The master device, user databases, and the transaction log are all stored on different partitions of the same physical device, and are all mirrored to a second physical device. Failure of either disk will not interrupt SQL Server users. The drawback is that applications with a lot of update transactions may be slower. There are other options for mirroring based on cost and performance trade-offs.
2	Use Views and stored procedures to enforce access control.	Restricts direct access to tables.

Informix Application Development Guidance

Item	Guidance	Rationale
1	Perform periodic consistency checking. Use either Onmonitor, Onstat, Onperf, Dbcockpit, or Oncheck to perform consistency checks.	Consistency checks help detect problems that might be caused by hardware or operating system errors or unknown problems within OnLine. Oncheck allows the DBA to do consistency checks on each database that is under an OnLine instance.
2	Create a new OnLine instance for each application running on the same host machine (it is also called multiple residency). This requires one entry for each OnLine instance in the /etc/hosts, /etc/services. and $INFORMIXDIR/etc/sqlhosts files. It also requires that the dbservernames and server numbers be unique.	Ensures that each application has its own set of configuration files and datafiles. Note that if there is more than one application on the same host, having separate instance for each may lead to performance degradation.
3	Each database within an application has its own dbspace.	Each database will have its own set of datafiles.
4	Shared databases have their own dbspace and data to be shared within individual tables is fragmented over dbspaces. Users can define a distribution scheme that specifies which table rows are in which dbspace. This was only data to be shared can be fragmented into the shared dbspace.	
5	Views and Stored Procedures are used.	Restricts direct access to tables.
6	When defining referential integrity constraints, use the CASCADES DELETE clause with caution.	The system table sysreferences lists the referential constraints placed on columns in the database. Check the column delrule, if its value is C, it means the delete rule is CASCADES DELETE. The CASCADES DELETE option deletes all child rows

when the parent row is deleted. Also a user just needs delete privilege on the parent table to be able to delete the parent row which in turn deletes the child rows as well.

Windows NT 3.5.1 Application Development Guidance

Item	Guidance	Rationale
1	Protection mode is turned on Windows NT Registry key.	
2	The application does not depend on the availability of the Guest account.	
3	The application does not require users to be members of the group "Administrators".	
4	The application can be installed by a user who is not a member of the group "Administrators."	
5	When an application copies a file, the ACL of the new file is set to the ACL of the original file or the ACL is set to an explicitly specified new ACL (i.e., the new file should not simply inherit the ACL of the new parent directory).	
6	When an application modifies a file owned by a user other than the user currently executing the application, the ownership of the file should remain unchanged after the modification.	
7	Application servers and services that take actions controlled by a user impersonate the user who initiated the actions.	
8	The application runs correctly with all directory and executable file permissions set to Everyone: RX Administrator: FULL System: FULL	
9	The application is compatible with planned firewall installations.	
10	The application installation or execution does not modify Registry Key ACLs.	
11	The registry keys set by the application installation process have ACLs set so that Everyone is only allowed:	

Query Value
Enumerate Subkeys
Notify
Read
Control

12	The application is scanned immediately before installation with a current virus checking program.	
13	If the site is configured as a domain, verify that a domain backup controller is available.	Access to the domain controller is required for most user activities and becomes a major point of failure.
14	If the site is configured as a domain, ensure that application servers are not hosted on domain controllers.	Login activities are frequent and essential. Application usage could tie up the server system or application maintenance could require the server system to be taken off-line. In addition application administrators may need administrator rights on the shared system, giving them access to the SAM database as well.
15	If the site is configured as a domain, ensure the domain controller and the domain backup controller are physically protected.	Domain controllers are a single point of attack for user capabilities. If any account with administrative rights is compromised, the attacker can change rights of any user on the network.